A collaborative approach for national cybersecurity incident management

Journal:	*Information and Computer Security*
Manuscript ID	ICS-02-2020-0027.R3
Manuscript Type:	Original Article
Keywords:	Information security, Conflict, Risk Management, Trust

A collaborative approach for national cybersecurity incident management

ABSTRACT

Purpose

Collaborative-based national cybersecurity incident management benefits from huge size of incident information, large-scale information security devices and aggregation of security skills. However, no existing collaborative approach has been able to cater for multiple regulators, divergent incident views and incident reputation trust issues that national cybersecurity incident management presents. This paper proposes a collaborative approach to handle these issues cost-effectively.

Design/Methodology/Approach

A collaborative-based national cybersecurity incident management architecture based on ITU-T X.1056 security incident management framework is proposed. It is composed of the cooperative regulatory unit with cooperative and third-party management strategies, and execution unit, with incident handling and response strategies. Novel collaborative incident prioritization and mitigation planning models that are fit for incident handling in national cybersecurity incident management are proposed.

Findings

Use case depicting how the collaborative-based national cybersecurity incident management would function within a typical ICT ecosystem is illustrated. The proposed collaborative approach is evaluated based on the performances of an experimental cyber-incident management system against two multistage attack scenarios. The results show that the proposed approach is more reliable compared to the existing ones based on descriptive statistics.

Originality/Value

The approach produces better incident impact scores and rankings than standard tools. The approach reduces the total response costs by 8.33% and false positive rate by 97.20% for the first attack scenario, while it reduces the total response costs by 26.67% and false positive rate by 78.83% for the second attack scenario.

Keywords: Incident management, national cybersecurity, information security management, collaborative approach, incident handling and response

1. Introduction

Globally, attackers have evolved sophisticated methods, which have made cyber-attacks difficult to combat. The 2018 threat report by Symantec Enterprise Security (Symantec, 2019) showed that the level of targeted, form-jacking, IoT, ransomware, cloud and election interference attacks have risen more than previous years. Thus, more effort is needed in security management to avert the losses in information systems and assets.

According to Ntouskas *et al.* (2011), security management is a continuous and systematic process of identifying, analysing, handling, reporting and monitoring operational risk of an organisation, while threat management is central to it (SensePost, 2011). The core objective of information security management is to implement the appropriate measurements to eliminate or minimize the impacts of threats such as incident and vulnerabilities in the organization.

Different information security management system specifications exist such as ISO/IEC 27000, ISO/IEC 27001, and ISO/IEC 27002. Both ITU-T and ISO/IEC jointly developed recommendation ITU-T X.1051(information technology, security techniques and information security management guidelines for telecommunications organizations based on ISO/IEC 27002), which establishes guidelines and general principles for information security management in telecommunications organizations. The standard is composed of other standards like ITU-T X.1056, which focuses on security incident management guidelines.

Security incident management involves incident handling and response services that help prevent incidents (Alberts *et al.,* 2004). The incident handling services include detection and reporting of incidents, correlation, categorization, prioritization, and assignment of events, and mitigation planning steps. The incident response involves the actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies.

Fighting security threats with only a local view is inherently difficult. Seigneur and Slagell (2009) briefly described collaborative security as: “instead of centrally managed security policies, nodes may use specific knowledge (both local and acquired from other nodes) to make security-related decisions”. The decisions must happen in a community in which nodes can contribute their efforts to make the decisions more effectively and reasonably. Nodes should collaborate with each other by sharing some information, analysis results and security related decisions. Collaborative security management system is therefore a joint effort between multiple security management systems.

Sharing of relevant incident information intelligence among multiple security management systems facilitates detection and prevention of large-scale cyberattacks in cost-effective manner across different collaborative security management systems (Staniford *et al.,* 2002). However, issues such as synergy, trust, standardization, analysis, and control must be addressed (Saklikar, 2013)

The different levels of collaborative security management include system-level security incident management (S-SIM) (Chen *et al.,* 2007; Chen, *et al.* 2013), organizational-level security incident management (O-SIM) (Ntoukas et al., 2011; Pan et al., 2016) and national-level security incident management (N-SIM) (Settanni *et al.,* 2017). S-SIM involves collaboration among computers and devices in single organization. It may involve single or multiple security managers, homogeneous or heterogeneous devices and an organizational security policy; O-SIM involves collaboration among security domains in a federated organization, with many partner organizations that share similar functions (Ntoukas *et al*., 2011). Each organization in the federation has one or more security manager and information security devices. N-SIM involves a chain of collaboration among individuals, organizations and regulators within a country, region, or continent, which in many cases involves multiple regulators, heterogeneous devices, varying functions, and divergent incident views. While S-

SIM and O-SIM may have the capability to pay attention to significant incidents (Weiss, 2015), N-SIM can provide better regulation, in-depth incident analysis and be made to pay attention to significant incidents through prioritization of incidents based on their impacts at the S-SIM and O-SIM levels and interdependencies (Settanni *et al.,* 2017). Therefore, N-SIM will be very beneficial to systems and organizations, most especially connected infrastructures. According to a PwC report, a successful cyber-attack on a telecommunications operator could disrupt service for thousands of phone customers, internet service for millions of consumers, cripple businesses, and shut down government operations (Lobel, 2014).

In concordance with the existing national cybersecurity incident management recommendations such as ENISA (2013), European Commission (2016), NIST (2018), and GC CSEMP (2018), this paper proposes an improved collaborative approach for national cybersecurity incident management.

2. National Cybersecurity Incident Management

National cybersecurity incident management enables the collection and processing of incident-related information most especially interdependent services and shared resources in global contexts (Amanowicz, 2020). It enables exchange of information, experience, and security devices, which lead to information heterogeneity, divergent incident views and incident reputation trust issues. In some cases, the challenges may be complicated by multiple regulations and conflicting guidelines.

Several standards, which support collaborative incident management have been developed to provide frameworks for sharing cybersecurity incident information. RFC 7970 Incident Object Description Exchange Format (IODEF) (Danyliw *et al.,* 2007) was developed as a legacy format for exchanging incident information. The problem with the framework is that it does not cater for integration of relevant information that are related to vulnerability, weakness, information security device and configuration updates. RFC 7203 IODEF for Structured Cyber Security Information (IODEF-SCI) (Takahashi, 2013) was developed as an extension to IODEF to cater for the missing information.

Other frameworks include RFC 6045 Real-time Inter-network Defense (RID) (Moriarty, 2012), which outlines a proactive inter-network communication method to facilitate sharing of incident data while integrating existing detection, tracing, source identification, and mitigation mechanisms. This provides a way to achieve higher security levels on networks. RID functions via request, acknowledgement, result, report, and query message types. MITRE Standards (Farnham, 2013) such as CybOX, STIX, TAXII were also developed. Cyber observable expression (CybOX) provides a standard for defining indicator details known as observables; structured threat information expression (STIX) provides a standard to define patterns of observables in context while trusted automated exchange of indicator information (TAXII) provides a standard to exchange cyber threat intelligence.

These standards have been applied to N-SIM in Settanni *et al.* (2017), which proposed a collaborative cyber-incident management system for European interconnected critical infrastructures based on the European cyber-security operation centres (SOCs). The national-level SOCs were responsible for correlating the security-related data, analysing, and providing support and mitigation strategies to organizational-level SOCs. Single national-level SOC was proposed for each substituent unit (country). The data collection and cross-SOC information exchange activities in the system were organized into data collection, data fusion, data sharing, data encryption and trust, collaboration while feature extraction and analysis was organized into incident system component and analysis model, with information entities, artefact extraction and resource linking. Other aspects of the system included incident visualization and mitigation. The incident handling process did not provide any mechanism for addressing the

incident reputation trust issue and show how the divergent views of incidents were aggregated. The system was evaluated with cyber-physical attack scenario on gas supply, but the outcomes were not presented. Common cybersecurity awareness of critical infrastructure was presented in Puuska *et al. (*2018). They designed a common operating picture system to monitor large-scale critical infrastructures. Joint Directors of Laboratories (JDL) data were fused to integrate different critical infrastructure systems with their dependency relations. This allowed for situational awareness of critical infrastructure and networks. Five levels of processes involving different JDL were performed such as pre-processing, object refinement, situation refinement, threat refinement, process refinement and cognitive refinement to predict the performance levels of operators.

Some other collaborative-based incident handling and response systems, which have functioned as O-SIM and S-SIM include Sequoia, a robust communication architecture for distributed internet-scale security monitoring systems, proposed by Kang *et al.* (2004). Sequoia supported regional and global sharing of monitored observations, collaborative decision-making among monitors, and timely delivery of security information to monitors. The system relied on certificate-based routing to ensure trust among parties. Sequoia's architecture supported aggregation, integration, and dissemination of blacklists using a publisher-subscriber paradigm. Sequoia comprised three key protocols: the monitor neighbour discovery protocol (MND) for topology-aware flat overlay among monitors to allow connection to nearby nodes(neighbours); distributed dominator selection protocol (DDS) that ensured that monitors met minimum requirements regarding trustworthiness and routing performance and the communication path discovery protocol (CPD) for discovering multiple delivery paths among nodes. Ullrich (2004) presented DShield, which aggregated firewall and intrusion detection system logs from global Internet. Each log entry representing one or more packets that violated a local rule was normalized. The entry included: time-detected, submitter's ID, count, source IP, source port, destination IP, destination port, protocol exploited, and flags. Ntoukas *et al.* (2011) proposed a collaborative network security management platform called Storm to improve security in distributed and complex information systems with critical data and services. The platform made use of advanced open source technologies and interactive software tools. The tool was applied to a port information system security and the results show the effectiveness of collaborative network security management in the distributed system. Chen *et al.* (2013) proposed a collaborative unified threat management system to mitigate botnets. The system consisted an effective collaborative unified threat management (UTM) and traffic probers. A distributed security overlay network with a centralized security centre leveraged by a peer-to-peer communication protocol was used in the UTM collaborative module. The security functions for the UTM were retrofitted to share security rules. A cloud-based security centre was used for network security forensic analysis. The cloud storage kept collected traffic data and enabled processing of data with cloud computing platforms to find the malicious attacks. Chen *et al.* (2014) proposed an architecture, mechanism design and system implementation of vCNSMS, a collaborative network security prototype system in multiple tenant's data centre network. The work demonstrated vCNSMS with a centralized collaborative scheme and deep packet security check. A security level-based protection policy was proposed for simplifying the security rule management for vCNSMS.

Pan *et al.* (2016) introduced HogMap, a novel software-defined network (SDN) infrastructure that simplified and incentivized collaborative measurement and monitoring of cyber-threat activity. HogMap integrated several novel SDN-enabled capabilities such as intelligent in-place filtering of malicious traffic, dynamic migration of interesting and extraordinary traffic and a software-defined marketplace where various parties can opportunistically subscribe to and publish cyber-threat intelligence services in a flexible manner. The system was implemented as SDN-based HoneyGrid, which spans traffic filtering,

traffic forwarding and connection migration. The result showed that SDN technologies greatly simplify the design and deployment of such globally distributed and elastic HoneyGrids. Wu and Wang (2018) developed a consensus protocol to implement the information sharing and fusion in a collaborative manner with the objective of achieving the maximum security for IoT systems. A game theoretical analysis framework was employed for the collaborative security detection by considering the confrontation between the defender and the attacker. The existence and uniqueness of the Nash equilibrium of game model with complete consensus were analysed. Then an iteration learning based calculation method was presented to determine the Nash equilibrium. Quantitative analysis was provided for the relationship between the Nash equilibriums of the game models in the cases of complete and incomplete consensus with infinite and finite number of iterations.

The review has shown that no collaborative-based national cybersecurity incident management system has addressed synergy, trust, standardization, analysis, and control in scenarios with multiple regulatory frameworks, heterogeneous devices, divergent incident views and incident reputation trust requirement.

Our work is therefore different from existing works based on the following contributions:

- creation of a collaborative framework for national security incident management, with multiple regulators
- provision of models to handle regulation conflicts among N-SIM regulators,
- development of trust-based multi-perspective incident handling and response models,
- provision of security incident management use cases for typical national cybersecurity.
- performance evaluation of the proposed national security incident management approach.

The remainder of the paper is organized as follows: Section 3 presents and describes the collaborative framework of national security incident management; Section 4 presents the models for the incident handling and response tasks; Section 5 presents the performance evaluation based of attack scenarios and surveys. Section 6 presents the use cases for the application of national cybersecurity incident management in Nigeria ICT ecosystem. The paper is concluded in Section 7.

3. Collaborative Framework for National Security Incident Management

In Figure 1, we present the framework of national security incident management, which is based on ITU-T X.1056 (Security Incident Management Guidelines for Telecommunications Organizations) because of its robustness in handling different cybersecurity incident management standards. The system consists National Control Unit (NC) with different abstractions and Security Incident Management Execution Unit (SIME).

Fig. 1. National Security Incident Management Framework

3.1 National Control Unit

The NC is composed of national security managers (security managers), different sets of regulatory guidelines and incident report monitor. Each security manager ensures that the incident security management guidelines of his regulatory agency is adhere to. The guidelines are made up of different rules for ensuring trust, synergy, policy compliance, standards, prompt analysis of incidents, recommendation of mitigation strategies and review of actions. The following strategies ensure the guidelines are not violated.

a. Cooperative Management Strategy: All the security managers are involved in the enforcement of trust and synergy, enforcement of policies and standards, analysis of incidents,

recommendation of mitigation strategies and review of actions. The shared key encryption scheme ensures that no individual or part of the security managers have full access control over the incident management process.

b. Third Party Management Strategy: A third-party auditor monitors and reviews all the activities of the security managers to ensure compliance with guidelines. He resolves regulation conflicts among the national security managers when there is breach at the cooperative management level.

The security managers aggregate the different views of the incident submitted by the S-SIM, O-SIM, and N-SIM which can be accessed via the incident report monitor. The N-SIM operator is in-charge of the data centre infrastructure; he updates the security managers about detected incidents. When a security manager observes a request alert at the monitor, he communicates with the other security managers to be able to decrypt the alert since the message can only be decrypted through shared key. The data is saved in encrypted format, which can only be decrypted using shared keys owned by the security managers using encryption scheme such as SunScreen SKIP (Oracle, 2010). Upon completion of incident response, the information is encrypted based on Attribute-based Encryption (Bethencourt *et al.*, 2007). Figure 2 illustrates the interaction among the components in the national control unit.

Fig. 2: National Control Unit

The incident views could be organized into five different levels of abstractions such as:

a. operator-level view, which is the highest level of abstraction. At this level, the profile of the participant security operator is known.
b. system-level view, which is the next lower level to the operator-level. At the level, the structural and some basic functional details of the information system is viewed.
c. asset-level view, which is the next lower level to the system-level. At this level, the details of the functions, services, and connectivity as well as updates of the components are viewed.
d. vulnerability-level view, which is next to the asset-level gives the details of flaws and threats that might likely violate the assets.
e. attack-level view, which is the lowest level of abstraction. At this level, the most probable paths of attacks given sets of mitigation measures can be observed.

3.2 Security Incident Management Execution Unit

The SIME has two components, which are the data centre and security incident management decisions components. The incident-related information is stored in the data centre using RFC 7203 IODEF-SCI (Takashi, 2013) template, because it provides detail incident-related information and it is cross-platform. Unstructured incidents-related information in text format can be submitted by the S-SIM, O-SIM and N-SIM operators but they are converted to a structured format by using natural language processing techniques to identify the incident and other information. The first step is to pre-process the texts using NLTK packages (Bird and Kliein, 2009), extract the n-gram weighted by term frequency inverse document format (Gaydhani *et al.,* 2018) and classify the data using Scikit learn packages (Pedregosa *et al.,* 2011). The data template for the incident-related information is presented in Table 1.

Table 1. Structured of Incident-related Information

The security incident management process lifecycle presented in Figure 3 involves the following incident handling and response steps:

a. Task Review: At this point, incident requests are reviewed at the beginning of security incident management, while recommendations are reviewed at the end of the process against the guidelines.
b. Incident Preparation: The incident features required for the subsequent stages are transformed to their usable format.
c. Incident Categorization and Correlation: This involves aggregation of incidents from different sensors and operators, with different incident names and incident reconstruction usually involving multi-step correlation to understand the attack patterns.
d. Incident Prioritization: The rating of the incident based on certain indices and computation.
e. Incident Assignment: The ranking of the incident according to their impacts and risks to systems at S-SIM, O-SIM and N-SIM such as {1, 2,3, …, N} or {Very Low, Low, Medium, High, …, M}
f. Mitigation Planning: Cost-effective mitigation and recovery response strategy are recommended against the attacks.
g. Incident Response: Cost-effective mitigation and recovery actions are implemented, and the performance is evaluated.

Fig. 3. Security Incident Management Process Lifecycle

4. Incident Handling and Response Strategies

The following models are used to carry out the incident handling and response steps:

4.1 Incident Categorization and Correlation

In this phase, the new incidents are reviewed, prepared, and categorized by aggregating them with existing incidents in the data centre and observing the attack patterns. If the incident has not been reported before, correlation take place using effective alert correlation strategy.

Several alert correlation strategies exist. Bayesian networks was used in Jemili *et al.* (2009), while Probabilistic Hidden Markov Model (HMM) in Haslum (2010). Data mining techniques were used for predictive attack plan recognition and intrusion prediction in Li *et al*. (2007), while it was combined with HMM in Farhadani *et al.* (2011). Because of the incompleteness and assumptions in Bayesian Networks and HMM and the incremental large volume of the incidents, the sequential association mining of Li *et al*. (2007) was adapted for the correlation.

However, rather than using only incident name to define incident, the trio of incident_name, source_IP and dest_IP address are used. Other features such as source_port, dest_ports, protocols, incident_ID are removed. The incidents are sorted in order of detect_time.

The average detection time is chosen as the window size. The Sequential Association Mining algorithms presented below are used to generate candidate attack sequences and interesting attack patterns, respectively.

CANDIDATE_SEQUENCE (Windowstep, Sequence)
// Generate every sequence of attack pattern
Step 1: Set WindowSize to P, SequenceSize to 1
Step 2: MaximumSequence Size to L, Sequence to empty, MaxIncidentSize to N
Step 3: Sort incidents based on their timestamps.

Step 4: Set the current WindowStep to 1
Step 5: Set Temp to empty, Set Incident Size
Step 6: IF IncidentSize < N
Step 5: IF WindowSize < L
Step 7: Increment SequenceSize by 1
Step 8: Add incident to Temp
Step 9: ENDIF
Step10: Add Temp to Sequence
Step11: Return WindowStep, Sequence
Step12: ENDIF

INTERESTING_SEQUENCE (Sequence)
//To find the interesting attack sequences
Step 13: Set WindowStep to 1, Threshold to T, Set TempLocation to 0, Temp to empty, InterestingSequence to empty
Step 14: Assign MinimumSupport to MinSup, WindowStep to Max
Step 15: IF WindowStep < Max
Step 16: Increment the WindowStep
Step 17: Add Sequence to Temp
Step 18: IF TempLocation != Temp
Step 19: Increment the TempLocation
Step 20: Compute the Support in Temp
Step 21: IF Support ≥ MinSup
Step 22: Compute the Confidence in Temp
Step 23: IF Confidence =1
Step 23: InterestingSequence ← Sequence
Step 24: ENDIF
Step 25: ENDIF
Step 24: Return Sequence
Step 25: ENDIF
Step 26: ENDIF

The support and confidence are estimated using the formulae below:

$$\text{Support (B)} = \frac{n(A \cap B)}{N} \quad (1)$$

$$\text{Confidence (B)} = \frac{n(A \cap B)}{n(A)} \quad (2)$$

Where

A is known as Antecedent and B is known as Consequent.
N is the number of incidents
n (A∩B) is the number of times A and B occurs together as sequence in the sequence table such that A is the antecedent and B is the consequent.
n (A) is the number of times the antecedent A occurs.

Based on the assumption that a once successful attack exploit would be exploited by an attacker in the near future than a none successful one; only the longest attack sequence (interesting attack pattarns), in which each step(stage) has confidence of 1(sequence that occur three times) are chosen to determine the actionable threat paths since the attack was replayed three times.

4.2 Incident Prioritization

Several incident prioritization strategies have been developed such as Caswell and Roesh (1998), Porras *et al.* (2002), Lee and Qin (2003), Alsubhi *et al.* (2008), Dondo (2008), Mell *et al.* (2009) and Jumaat (2012). The only collaborative-based incident prioritization strategy was Yu *et al.* (2004) developed for multiple IDS products. It combined intelligent agents and knowledge-based alert evaluation system. They evaluated the alert priority based on asset characteristics; however, the strategy neither considered the reputation of the incidents nor made provision for task review.

4.2.1 Incident Reputation Handling

Apart from encryption-based privacy, incident reputation is important in the estimation of the impact of incidents. The security managers critically examine the level of reputation of the participant security operators, communication media, information security devices and other incident sources based on trust in compliance with ITU-T Y.3052 (Overview of trust provisioning in information and communication technology infrastructures and services) and apply it to prioritization of incidents.

In social science research, integrity, ability, benevolence and trust propensity have been proven to be indicators of trust among human beings (Kee and Knox, 1970; Barber, 1983; Butler, 1991 and Mayer *et al.,* 1995). The communication media reputation depends on confidentiality, integrity and availability (Whitman and Mattord, 2004), while the trust of a data source depends on reliability, integrity and comprehensibility of the Information provided (Hu and Yang-Li, 2007; Nath *et al.,* 2010). In this study therefore, we evaluate trust based on integrity, ability, benevolence and trust propensity indices for security operators; confidentiality, integrity and availability indices for communication media; and integrity, comprehensibility and reliability for incident-related data sources. Table 2 presents the trust classes with the indicators and their descriptions.

Table 2: Trust Classes, Indicators and their Descriptions

We define trust, *T* as the measure of belief for incident, x and mass function (M_j) as the sum of the measures of the indicators (d_i) as presented in (3)-(5).

$$M_j = \sum_{i=1}^{10} d_i \quad (3)$$

since the indicators are 10.

$$\text{Where} \quad 0 \leq M \leq 1 \quad (4)$$

$$\text{And} \quad 0 \leq d_i \leq 0.1 \quad (5)$$

To combine the mass function, rules of combinations such as sum, product, average, tan-h, Rough Set, Fuzzy Set or Bayesian rules could have been used. However, they require scores or probabilities for each question of interest which are not actualisable in network security field, in which many information are collected through indirect means. Dempster-Shafer method is used to obtain degrees of belief of one evidence from subjective probabilities for a data source. The Dempster-Shafer theory of belief function is a generalization of the Bayesian theory of subjective probability(Shafer, 1976). The advantage over Bayesian Theory is that the degrees of belief for one question can be based on the probabilities for a related question. The Dempster-Shafer theory consists of hypotheses, pieces of evidence and data sources. The hypotheses represent all the possible states (evidence assignments). It is required that all

hypotheses are elements (singletons) of the frame of discernment, which is given by the finite universal set Ω. The set of all subsets of Ω is its power set 2^{Ω}. The pieces of evidence are the qualitative scores or observations, which may occur within a system.

The measure of Belief is derived from the combined basic assignments of the mass function (M). In this task, the Dempster's Rule (Shafer, 1976) that combines multiple belief functions through their basic probability assignments is used. These belief functions are defined on the same frame of discernment based on independent arguments or bodies of evidence. The Dempster's Rule of combination is purely a conjunctive operation (AND). Specifically, the combination (called the joint $M_{12\ldots n}$) is calculated from the aggregation of probability assignment functions M_1, M_2, …, M_n as presented in (6)-(10). The numerator represents the accumulated evidence for the sets *B, C, ..., Z*, which supports the hypothesis *A*, and the denominator is the sum of the amount of conflict among the sets.

$$T(x) = M_{12\ldots n}(A) \quad (6)$$

$$\text{When} \quad A \neq \emptyset ; \quad (7)$$

$$\text{and} \quad M_{12\ldots n}(\emptyset) = O \quad (8)$$

$$M_{12\ldots n}(A) = \frac{\sum_{B \cap C \ldots \cap Z = A} M_1(B) M_2(C) \ldots M_n(Z)}{1 - K} \quad (9)$$

$$K = \sum_{B \cap C \ldots \cap Z = \emptyset} M_1(B) M_2(C) \ldots M_n(Z) \quad (10)$$

where *B*, *C*, *A* $\subseteq$ A. M are the mass functions. A is the hypothesis.

4.2.2 Impact of Incidents

Because impact of incident depends on the attack capability and victim vulnerability, attacker and victim-based intrusion perspectives (McHugh *et al.,* 2001) are used to model incident for in-depth analysis of incidents. Table 3 indicates the attacker's perspectives, the criteria considered in the perspectives and how the criteria are assessed, while Table 4 indicates the victim's perspectives, the criteria considered in the perspectives and how the criteria are assessed. The criteria are assessed on 1-to-3 scale. The attacker-based perspectives are based on how the attacker would view the vulnerable system, while the victim-based perspectives are based on how the victim would view the attack. We combine both perspectives to prioritize or estimate the impact of incidents in systems.

Table 3: Attacker-centric Perspectives, Criteria and Scales

Table 4: Victim-centric Perspectives, Criteria and Scales

The impact of an incident is evaluated using the perception scores weighted by trust as presented in (11)-(18). The following steps are followed.

4.2.2.1 Trust Normalization

The maximum trust for threat, x for the criteria is normalized so that the sum is equal to 1.

$$T_k = \text{Normalized } (T(x)) = \frac{T_i}{\sum_{j=1}^{n} T_j} \quad (11)$$

Where T_k = *Max (T(x))* (12)

4.2.2.2 Expected Value for each incident perspective

The expected value for incident perspective (E) is the weighted sum of the products of trust (T_k) and perspective score (S_k)

$$E(P) = \frac{\sum_{k=1}^{c} T_k S_k}{\sum_{k=1}^{c} T_k} \quad (13)$$

$$\text{When } \sum_{k=1}^{c} T_k = 1; \quad (14)$$

$$E(P) = \sum_{k=1}^{c} T_k S_k \quad (15)$$

4.2.2.3 Impact of Incident

The impact of an incident for attacker's perspective (R_A) is the sum of the expected values for all the attacker's incident perspectives divided by asset ranking in terms of importance (Q).

For all m, n, N $\subseteq$ N such that m < n, Then

$$R_A = \frac{\sum_{l=1}^{m} E_i}{Q} \quad (16)$$

Where $1 \leq m \leq 3$ (m is attacker's perspectives)

The impact of an incident for victim's perspective (R_v) is the sum of the expected values for all the victim's
incident perspectives divided by asset ranking (Q)

$$R_v = \frac{\sum_{l=4}^{n} E_i}{Q} \quad (17)$$

Where $4 \leq n \leq 6$ (n is victim's perspectives)

$1 \leq Q \leq L$ (The highest Q is 1 and the lowest is L)

The impact of incident (R(x)) is the sum of impact for attacker's perspective and victim's perspective for incident, x.

Thus, $R(x) = R_A + R_V$ (18)

4.2.3 Incident Assignment

The incident with impact scores, R that are above R_z ($R > R_z$) are classified as high; those below R_z but greater or equal to R_y ($R_z > R \geq R_y$) are medium; those below R_y but greater or equal to R_x ($R_y > R \geq R_x$) are low; and those below R_x are very low. Also, an incident is ranked high when the incident has no impact score.

4.2.4 Mitigation Planning

Hillson (1999) Risk Control Strategy is adapted in this study because of its popular usage and effectiveness. The strategies are presented as follows with its flowchart in Figure 4.

a. Avoid: The action to be taken is to enable both detection and prevention layer.
b. Transfer: The action to be taken is to improve detection and prevention layer capability
c. Mitigate: The action to be taken is to enable detection layer and disable prevention layer.
d. Accept: The action to be taken is to disable detection and prevention layers.

Fig 4. System Flow Chart for Mitigation Planning

4.2.5 Incident Response

At this stage, the incident response actions are taken, and the performance is evaluated based on response cost and benefit. The incident response model is a seven-tuple (X, D, P, M, A, C, B) where:

X: a finite set of t incidents, $X= \{x_1, x_2,\ldots,x_t\}$ subject to $M = \{M_1, M_2, M_3, M_4\}$.
D: a finite set of n assets $(d_1, d_2, \ldots, d_{n)}$ at the S-SIM, O-SIM and N-SIM levels.
P: a finite set of active u assets $(p_1, p_2, \ldots, p_{u)}$ for active S-SIM, O-SIM and N-SIM.
M: a finite set of w enabled security options $(m_1, m_2, \ldots, m_{w)}$ at the S-SIM, O-SIM and N-SIM levels.
A: incident assignment shows the rank of the incidents. It includes very low, low, medium and high.
C: response cost is sum of the cost of avoidance, transfer, mitigation and acceptance. The cost factor in USD per threat for avoidance is set at 40USD, transfer is set at 30USD, mitigation is set at 20USD, while acceptance is set at 10USD.
B: incident response benefit is the overall impact of response actions on the incidents, which can be based on false positive rate, detection rate, accuracy, f1-score, etc.

5. Performance Evaluation of the Collaborative Approach

The proposed collaborative approach was evaluated based on the performances of an experimental cyber-incident management system against two multistage attack scenarios.

5.1 Cyber-incident Management System's Testbed

The cybersecurity incident management system's testbed is depicted in Figure 5. The testbed consisted routers and switches as well as firewall, network and host-based intrusion detection systems, which were operated by N-SIM operators. At each O-SIM (SP), firewall, network and host-based intrusion detection systems were installed. The O-SIM network operated over four subnets: 10.1.0.128/27, 10.1.0.160/27, 10.1.0.192/27 and 10.1.0.224/27 each managed by an O-SIM operator.

Fig. 5: Structure of the cyber-incident management system's testbed

5.2 Attack Scenarios

Two multistage attacks were used to evaluate the proposed approach.

5.2.1 First Attack Scenario

We set up an attack targeted at CVE-2012-4681(NVD, 2012) against four O-SIM, one of which consisted three S-SIM, with Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 6. The four phases of the attack scenario are as follows:

a. Connect to the Victims
b. Scan the operating systems for exploitable vulnerability
c. Attempt to exploit CVE-2012-4681
d. Exploit CVE-2012-4681

The incident alerts of the sensors for the attacks were monitored at the O-SIM level through incident monitoring tools. Figure 6 indicates some instances of the intrusion detection system alerts for the first attack scenario as observed at the O-SIM operator level through Security Onion (Burks, 2014). The alerts and other information were submitted to the data centre through different communication media. After analysis of the report by the security managers, other incident information related to the vulnerability previously in the data centre were fused with the incidents using natural language processing technique (Settani *et al.,* 2017).

Fig. 6. Sample Alerts

The following sequence of incidents, which reflect the attack stages for first attack scenario as generated from incident categorization and correlation process is presented in Table 5. The result showed that only a host (10.1.0.135) was successfully attacked.

Table 5: Attack Stages for First Attack Scenario

5.2.2 Second Attack Scenario

In order to benchmark the model, the publicly available LLDOS 1.0 Inside exploits in four critical subnets: 172.16.112.0/24, 172.16.113.0/24, 172.16.114.0/24 and 172.16.115.0/24 (LLDOS 1.0, 2000) created by MIT Lincoln Lab in 2000 were filtered and merged with DARPA 1999 (LLDOS 1.0, 2000) background data collected on Monday of the first week. The five phases of the attack scenario are as follows:

a. IPsweep of the AFB from a remote site
b. Probe of live IP's to look for the sadmind daemon running on Solaris hosts
c. Breakins via the sadmind vulnerability, both successful and unsuccessful on those hosts
d. Installation of the trojan mstream DDoS software on three hosts at the AFB
e. Launching the DDoS

The incident alerts of the sensors for the attacks were monitored at the O-SIM level through incident monitoring tools. The alerts and other information were submitted to the data centre through different communication media. After analysis of the report by the security managers, other incident information related to the vulnerability previously in the data centre were fused with the incidents using natural language processing technique.

The following sequence of incidents, which reflect the attack stages for LLDOS 1.0 Inside exploits as generated from incident categorization and correlation process is presented in Table 6. This reflected the description in DARPA (2014). Different bots were applied at the reconnaissance IPsweep and scanning phases as shown in stage 1 and stage 2. It showed that after a successful exploit of sadmind vulnerability in a host 172. 16.115.20 of a particular

subnet, the attacker performs pings host 172.16.113.204 in another subnet. This conforms to the description in LLDOS 1.0 (2000)

Table 6: Attack Stages for Second Attack Scenario

To evaluate the incident prioritization model, we adopted the ranking scales of very low (A<5), low (8>A≥5), medium (12>A≥8) and high (A≥12) for the proposed N-SIM approach. However, the ranking scale for Snort (Caswell and Roesh, 1998) is from 1 (very low), 2 (low), 3 (medium) and 4(high), while Common Vulnerability Scoring System (CVSS) (Mell *et al*., 2009) is none (0), low (0.1-3.9), medium (4.0-6.9), high (7.0-8.9) and critical (9.0-10.0).

Table 7 and Table 8 present the outcomes of the incident prioritization model for the first and second attack scenarios, respectively compared to CVSS and Snort. Table 7 showed that for N-SIM, five incidents have low rank, while one incident has very low rank with varying scores, unlike Snort, which ranked all the incidents as low, with the same risk score of 2. CVSS, was worst with the score of 0 because all the incidents are not known to it. Table 8 shows that for N-SIM, seven incidents have very low ranks, one has low rank, three have medium ranks and one has high rank. N-SIM ranked incidents with or without CVE identification. In fact, four of the five incidents above very low rank have CVE-ID above high ranks, which signify the correctness of the proposed approach. Snort was poor having ranked IPsweep and probe exploits higher with medium ranks than break-in and DoS exploits, while CVSS was poor because it could rank only five incidents out of the twelve. Comparing the ranking of the proposed approach to the ranking of Snort using Spearman's correlation, r = 0.79 and p = 0.2 were obtained for first attack scenario, which showed that the ranking was positively significant at p>0.05. For second attack scenario, the results are r = -0.45 and p = 0.16, which showed that the ranking were negatively significant compared to Snort. The negative correlation was due to the poor prioritization by Snort, which ranked IPsweep and Probe attack exploits high and high priority exploits low. The proposed approach reflected the attack description in LLDOS 1.0 (2000) based on the ranks.

Table 7. Incident Prioritization Results for N-SIM Approach, CVSS, and Snort for First Attack Scenario

Table 8. Incident Prioritization Results for N-SIM Approach, CVSS, and Snort for Second Attack Scenario

In Table 9, the response cost for the first attack scenario based on the mitigation strategy showed that the proposed collaborative approach incurs the lowest cost of $110, followed by Snort with $120 and CVSS with $240. In Table 10, the response cost for the second attack scenario based on the mitigation strategy showed that the proposed collaborative approach incurs the lowest cost of $220, followed by Snort with $470 and CVSS with $300. Both tables show the response cost factors for the incidents and the total costs estimated as sum of response costs. Figure 7 and Figure 8 indicate the total response costs for the first and second attack scenario, respectively. In Figure 7, the proposed approach incurred lesser total response cost (cost ratio = 0.917, cost difference = -8.33%) in comparison with Snort, unlike CVSS that doubles the cost (cost ratio =2, cost difference = +100%). In Figure 8, the proposed approach incurred lesser total response cost (cost ratio = 0.733, cost difference = -26.67%) in comparison with Snort, unlike CVSS that almost doubles the cost (cost ratio = 1.567, cost difference = +56.67%). By replaying the attack against incident response configurations, the false positive

rate reduced from 99.15% to 2.78% for the first attack scenario and 99.97 to 21.16% for the second attack scenario.

Fig. 7. Total Response Cost for First Attack Scenario in Comparison with Snort

Fig. 8. Total Response Cost for Second Attack Scenario in Comparison with Snort

In Table 9, the performance comparison chart between the proposed N-SIM approach, Settani *et al.* (2017) and Puuska *et al.* (2018) is presented. The chart shows that the N-SIM approach is unique because it supports multiple regulators, divergent incident views and reputation trust, in comprehensive manner.

Table 9: Performance Comparison Chart for National Cybersecurity Incident Management Set-ups

6. Application to National Cybersecurity Platforms

6.1 The Nigerian ICT Ecosystem

6.1.1 Background of the Nigerian Information and Communication Technology Sector

The Nigeria ICT ecosystem has over the years suffered from poor regulation and synergy (Omotoso and Muyiwa, 2016) at the regulatory and service provider level. The Nigeria ICT sector is dominated by mobile networks operators and its associated value-added services, the device sales and distribution, the equipment sales and distribution and software sales and distribution, which are regulated by Nigerian Communications Commission (NCC) and National Information Technology Development Agency (NITDA).

The NCC is charged with the responsibility of regulating the supply of telecommunications services and facilities, promoting competition, and setting performance standards for telecommunication services in Nigeria (NCA Act, 2003), while NITDA statutorily develops regulations for electronic governance, monitoring of the use of information technology, electronic data interchange and other forms of electronic communication transactions (NITDA Act, 2007). In 2015, NCC released strategic vision plan for the period between 2015 and 2020 to provide comprehensive roadmap within the telecoms industry to promote innovation, investment, competition, consumer empowerment, and improve quality of service. However, much has not been achieved and there have been controversies about conflict in the regulations of NCC and NITDA (Elebeke, 2019).

Presently, the Nigerian ICT market has moved from a decade of year-on-year growth, to a period of stagnation from poor policy and incentives, besides the subscription rate (Omotoso and Muyiwa, 2016). These have forced many investors out of market. Much as these problems exist, there is need to strengthen the operating environment in order to sustain the previous growth trajectory and encourage a robust digital economy. A key area to consider is improvement of cyber-security systems, which will help mitigate the loss.

CBN-NEFF (2019) showed that electronic bank fraud cases in Nigeria have risen to 5.571 billion naira from 2016 to 2018. The report showed that the major electronic channels used to perpetrate fraud were automated teller machines, point-of-sale and mobile platforms. However, Nigeria ICT ecosystem is confronted with inadequate information security devices, scarcity of skilled security managers and poor cyber-security management frameworks which have made the ICT sector susceptible to increased cyber-threats.

6.1.2 Use Case

Based on the description with two regulators, national security incident management use case with two regulators is formulated for Nigeria ICT sector as follows:

6.1.2.1 National Control (NC)

The NC has telecommunication security manager, which is under the purview of NCC and electronic data security manager, which is under the purview of NITDA. The telecommunication security manager is responsible for ensuring telecommunication trust and synergy, compliance with telecommunication policy and standards, analysis of telecommunication incident and requests, offering of control and mitigation strategy advices on telecommunications and review of telecommunications aspects of security incident management execution actions. The electronic data security manager is responsible for ensuring electronic data (software) trust and synergy, compliance with data (software) policy and standards, analysis of software incident and requests, offering of control and mitigation strategy advices on electronic data (software) and review of electronic data (software) aspects of security incident management execution actions. Both collect and aggregate the different views of the S-SIM, O-SIM and N-SIM. In any case of conflict, the Ministry of Communication and Digital Economy (MCDE) (Pantami, 2020) serves as the third-party auditor.

6.1.2.2 Security Incident Management Execution (SIME)

The data centre is built on network infrastructure connected to operator service providers (S-SIM) and two national security managers (NCC and NITDA). Figure 9 presents a feasible use case for the implementation of the requirements within the Nigeria ICT ecosystem.

Fig. 9. Use Case for Cybersecurity Incident Management in Nigerian ICT Ecosystem

7. Conclusion

In this paper, we have presented a collaborative approach for national cyber-security incident management that supports multiple regulatory systems. The approach addressed paucity of incident information, inadequate information security devices, scarcity of skilled security managers and limitations of the existing cyber-security incident management frameworks. We formulated guidelines for integrating system, organizational and national security incident management domains based on ITU-T X.1056 with different views of incidents. Conflict between regulators was handled by cooperative and third-party management strategies. Strategies for managing heterogeneity and diverse perspectives were also formulated. The incident privacy and reputation trust bottlenecks were addressed by proposing shared key encryption scheme and web-of-trust, which was based on standard trust indices.

The collaborative approach was evaluated using two attack scenarios. A use case was also examined using Nigeria ICT ecosystem, with two ICT regulators as case study. The results showed that our approach is more realistic due to its dynamism, ability to prioritize known and unknown incidents. Furthermore, the response costs reduced by 8.33% and 26.67% for first and second attack scenarios, respectively and false positive reduced by 97.20% and 78.83%, respectively using Snort. Overall, the comparison of the proposed collaborative approach with

existing approaches showed that the proposed approach was better in terms of in-depth analysis.

In future, a national incident management system will be implemented in real-life based on the approach. The effectiveness of the system in handling conflicts and trusts will be evaluated empirically.

References

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., Zajicek, M. (2004) "Defining Incident Management Processes for CSIRTs: A Work in Progress". Technical Report CMU/SEI-2004-TR-015 ESC-TR-2004-015, Carnegie Mellon Software Engineering Institute.

Alsubhi, K., Al-Shaer, E. and Boutaba, R. (2008) "Alert Prioritization in Intrusion Detection Systems", Proceedings of the IEEE Network Operations and Management Symposium, Salvador, Brazil, pp. 33-40.

Amanowicz, M. (2020) "Towards Building National Cybersecurity Awareness", Intl Journal of Electronics and Telecommunications, Vol. 66, No. 2, PP. 321-326

Barber, B. (1983) "The logic and limits of trust", New Brunswick, NJ: Rutgers University Press.

Bethencourt, J., Sahai, A. and Waters, B. (2007) "Ciphertext-Policy Attribute-Based Encryption", in 2007 IEEE Symposium on Security and Privacy(SP'07).

Bird, S. and Kliein, E. (2009) "Analyzing Texts with Natural Language Toolkit: Natural Language Processing with Python", First. Edition, O'Reilly, California.

Burks, D. (2014) "Peel Back the Layers of your Networks in Minutes", Security Onion, Available at: https://resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_90218.pdf (accessed 10 April, 2015)

Butler, J. K., (1991) "Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory", Journal of Management,*17,* 643–663.

Cardenas, A.A, Baras, J.S. and Ramezani, V. (2004) "Distributed Change Detection for Worms, DDoS and other Network Attacks" in Proceedings of the 2004 American Control Conference, Boston, Massachusetts, June 30 -July 2, 2004.

Caswell, B. and Roesch, M. (1998) "Snort: The open source network intrusion detection system", Available at: http://www.snort.org (accessed 10 April, 2014)

CBN-NFF. (2019) "Annual Report 2018: Nigeria Electronic Fraud". Available at: https://www.cbn.gov.ng/Out/2019/CCD/NeFF. (accessed 10 November, 2019).

Chen, Y., Hwang, K. and Ku, W. (2007) "Collaborative Detection of DDoS Attacks over Multiple Network Domains", IEEE Transactions on Parallel and Distributed Systems, TPDS-0228-0806.

Chen, Z., Han, F., Cao, J., Jiang, X., and Chen, S. (2013) "Cloud Computing-Based Forensic Analysis for Collaborative Network Security Management System", Tsinghua Science and Technology, Volume 18, Number 1, pp40-50.

Chen, Z., Dong, W., Li, H., Cao, J., Zhang, P. and Chen, X. (2014) "Collaborative Network Security in Multi-Tenant Data Center for Cloud Computing", Tsinghua Science & Technology, 19(1):82-94.

LLDOS 1.0 (2000) 2000 DARPA Intrusion Detection Scenario Specific Datasets. Available at: https://www.ll.mit.edu/r-d/datasets/2000-darpa-intrusion-detection-scenario-specific-datasets. (accessed 21 May, 2020)

Dondo, M. (2009) "A Fuzzy Risk Calculations Approach for a Network Vulnerability Ranking System", DRDC Ottawa Defence R&D Canada – Ottawa, Technical Memorandum DRDC Ottawa TM 2007-090.

Elebeke, E. (2019) "NCC Regulation not in Conflict with Nigeria Data Protection Regulation – NITDA" Vanguard, Available at: https://www.vanguardngr.com/2019/10/ncc-regulation-not-in-conflict-with-nigeria-data-protection-regulation-nitda/(accessed 10 January, 2020)

ENISA (2013) "Detect, Share, Protect Solutions for Improving Threat Data Exchange among CERTs", European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs (accessed 8 July, 2019)

European Commission (2016) "Proposal for a directive of the european parliament and of the council concerning measures for a high common level of security of network and information systems across the union", Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF (accessed 8 July, 2019)

Farhadi, H., AmirHaeri, M. and Khansari, M. (2011) "Alert Correlation and Prediction Using Data Mining and HMM", The ISCInt'l Journal of Information Security, Volume 3, Number 2 pp. 77-101, Available at: http://www.isecure-journal.org (accessed 13 March, 2012)

Farnham, G. 2013. Tools and Standards for Cyber Threat Intelligence Projects. GIAC (GCPM) Gold Certification.

Gaydhani, A., Doma, V., Kendre, S and Bhagwat, L. (2018) "Detecting Hate Speech and Offensive Language on Twitter using Machine Learning : An N-gram and TFIDF based Approach." IEEE International Advance Computing Conference 2018.

GC CSEMP (2018) "Government of Canada Cyber Security Event Management Plan", Treasury Board of Canada Secretariat**.** Available at: https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html (accessed 26 July, 2019)

Haslum, K. (2010) "Real-time network intrusion prevention", Doctoral theses at NTNU, 2010:168.

Hillson, D. (1999) "Developing Effective Risk Responses", Proceedings of the 30th Annual Project Management Institute 1999 Seminars & Symposium, Philadelphia, Pennsylvania, USA.

Jemili, F., Zaghdoud, M. and Ahmed, M.B. (2009) "Hybrid Intrusion Detection and Prediction multiAgent System, HIDPAS", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 5, No.1.

Jumaat, A. N. B. (2012) "Incident Prioritization for Intrusion Response", University of Plymouth, Unpublished Ph.D. Thesis.

Kang, X., Zhou, D., Rao, D., Li, J. and Lo, V. (2004) "Sequoia – A Robust Communication Architecture for Collaborative Security Monitoring Systems", Available at: http://netsec.cs.uoregon.edu/research/sequoia.php (accessed 4 April, 2014)

Kee, H. W., & Knox, R. E. (1970) "Conceptual and methodological considerations in the study of trust and suspicion", Journal of Conflict Resolution, 14, 357–366.

Lee, W. and Qin, X. (2003) "Statistical causality analysis of INFOSEC alert data. Proceedings of the Recent Advances in Intrusion Detection", Pittsburgh, PA, USA, Vol. 2820/2003, pp. 73-93.

Li, Z., Lei, J., Wang, L. and Li, D. (2007) "A Data Mining Approach to Generating Network Attack Graph for Intrusion Prediction", Computer Communications 29.

Lobel, M. (2014) "*The Global State of Information Security Survey 2014*", PwC US, Available at: www.pwc.com/giss2014(accessed 26 July, 2019)

Locasto, M.E., Parekh, J.J., Keromytis, A.D., Stolfo, S.J. (2005) "Towards Collaborative Security and P2P Intrusion Detection", in Proceedings of the 2005 IEEE Workshop on Information Assurance and Security T1B2 1555 United States Military Academy, West Point, NY, 15.

Mayer, R. C., Davis J. H., and Schoorman F. D. (1995) "An Integrative Model of Organisational Trust", Academy of Management Review, 20, 709–734.

McHugh, J., Christie, A. and Allen, J. (2001) "Intrusion Detection1: Implementation and Operational Issues. CROSSTALK", The Journal of Defense Software Engineering, Software Engineering Institute, Computer Emergency Response Team/Coordination Centre.

Mell, P., Scarfone, K. and Romanosky, S (2009), "A Complete Guide to the Common Vulnerability Scoring System Version 2.0", Available at: http://www.first.org/cvss/cvss-guide.html (accessed 1 May, 2014)

Moriarty, K. (2012) "Real-time Inter-network Defense (RID)", RFC 654, Available at: www.ietf.org (accessed 1 April, 2014)

NCA Act (2003) "Nigeria Communications Act. Federal Republic of Nigeria Official Gazette", Vol. 90, No. 62, ppA287-A349.

NIST (2018) "Framework for improving critical infrastructure cybersecurity Version 1.1.". Available at: https://doi.org/10.6028/NIST.CSWP.04162018 (accessed 8 June, 2019)

NITDA Act (2007) "National Information Technology Development Agency Act", The Federal Republic of Nigeria Official Gazette, Vol. 94, No. 99.

Ntouskas, T., Pentafronimos, G. and Papastergiou, S. (2011) "STORM - Collaborative Security Management Environment. Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication", Lecture Notes in Computer Science Volume 6633, 2011, pp 320-335.

NVD (2012) "CVE-2012-4681 Details", National Vulnerability Database, Available at: https://nvd.nist.gov/vuln/detail/CVE-2012-4681 (accessed 3 February, 2019)

Omotoso, K.O. and Muyiwa A.C. (2016) "Prospects of Nigeria's ICT Infrastructure for E-Commerce and Cashless Economy", British Journal of Economics, Management & Trade, 2016, 13(2): 1-10.

Oracle (2010) "SunScreeen Skip Release 1.5.1", Oracle Cooperation. Available at: https://docs.oracle.com/cd/E19047-01/sunscreen151/806-5397/howskipworks-4/index.html (accessed 26 July, 2019)

Pan, X., Yegneswaran, V., Chen, Y., Porras, P., and Shin, S. (2016) "HogMap: Using SDNs to incentivize collaborative security monitoring", ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization, SDN-NFV Security 2016 - New Orleans, United States.

Pantami, I. (2020) "The Federal Ministry of Communication and Digital Economy" , Federal Republic of Nigeria. Available at: https://www.commtech.gov.ng/ (accessed August 5, 2020)

Pedregosa, F., Varoquaux G., Gramfort, A., Michel, V. and Thirion, B. (2011) "Scikit-learn: Machine Learning in Python", Journal of Machine Learning Reserch 12, 2825–2830.

Porras, P.A., Fong, M.W. and Valdes, A. (2002) "A mission-impact-based approach to INFOSEC alarm correlation", Proceedings of the 5th International Symposium Recent Advances in Intrusion Detection, Zurich, Switzerland, Vol. 2516, pp. 95-114.

Puuska, S, Rummukainen, L., Timonen, J., Lääperi, L., Klemetti, M., Oksama, L., and Vankka, J. (2018) "Nationwide critical infrastructure monitoring using a common operating picture framework", International Journal of Critical Infrastructure Protection, vol.20, 2018, pp. 28 – 47.

Saklikar, S. (2013) "Sharing Threat Intelligence Analytics", RSA Conference, Asia-Pacific, CLT-05 Intermediate Class.

Seigneur J. and Slagell A. (2009) "Collaborative Computer Security and Trust Management", IGI Global, Hershey, New York.

SensePost (2011) "Sense Modelling Threat Modelling", Available at: http://www.slideshare.net/sensepost/corporate-threat-modelling (accessed 4 April, 2014)

Settannia, G. , Skopika, F., Shovgenyaa, Y. , Fiedlera, R., Carolanb, M., Conroyb D., Boettingerc, K., Gallc, M., Brostc, G., Poncheld, C., Hausteind, M., Kaufmannd, H., Theuerkaufe, K. , and Ollif, P. (2017) "A collaborative cyber incident management system for European interconnected critical infrastructures". Journal of Information Security and Applications 34, pp 166-182.

Shafer, G. (1976) "A Mathematical Theory of Evidence", Princeton University Press, New Jersey.

Staniford, S., Paxson, V., and Weaver, N. (2002) "How to Own the internet in your spare time", in Proceedings of the 11th USENIX Security Symposium (Security '02), 2002.

Symantec (2019) "Internet Security Threat Report", Volume 19, Available at: www.symantec.com/content (accessed 5 June, 2019).

Takahashi, T. (2013) "IODEF-extension for structured cybersecurity information". Available at: http://tools.ietf.org/html (accessed 4 April, 2014)

Ullrich, J. (2004) "Dshield home page", Available at: http://www.dshield.org/ (19 January, 2014)

Wang, J. and Zhao, L. (2006) "Experimental Design for Attack Scenario Traces to validate Intrusion Detection Alert Correlation", WSRC Paper 2006/4-1, Whartson-SMU Research Centre.

Weiss, N.E. (2015) "Legislation to facilitate cybersecurity information sharing: economic analysis", Congressional Research Service 7-5700

Whitman, M. E. and Mattord, H. J. (2004) "Management of Information Security", Thompson Course Technology, Available at: http://www.thomsonrights.com (accessed 19 January, 2014)

Wu, H. and Wang, W. (2018) "A Game Theory Based Collaborative Security Detection Method for Internet of Things Systems", IEEE Transactions on Information Forensics and Security, (99):1-11·

Yu, Y, Ramana-Reddy, Y.V, Selliah, S., Reddy, S. and Bharadwai, V. (2004) "A collaborative architecture for intrusion detection systems with intelligent agents and knowledge-based alert evaluation", Conference Proceeding on Computer Supported Cooperative Work in Design. The 8th International Conference on Volume: 2

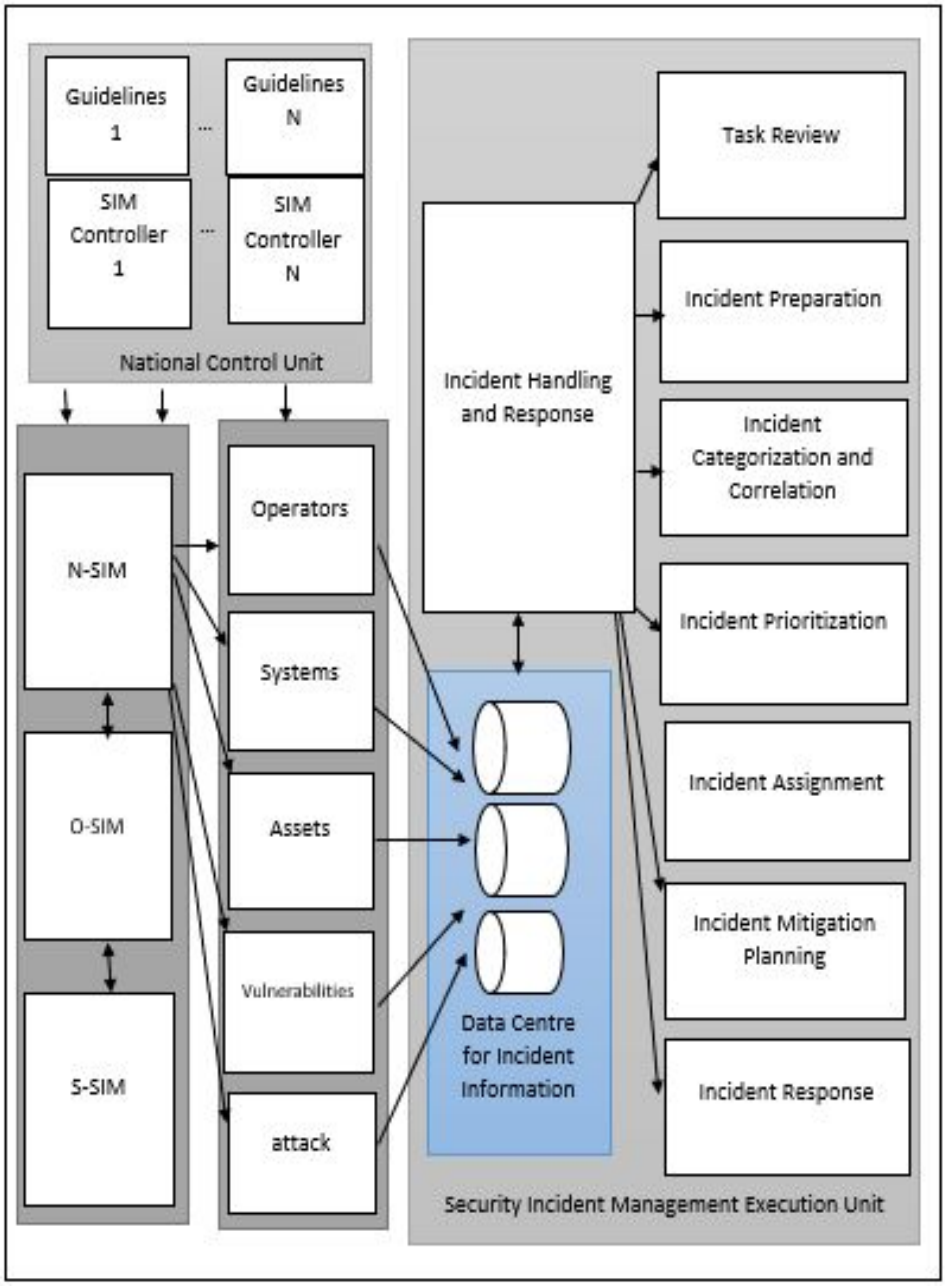

Fig. 1. National Security Incident Management Framework

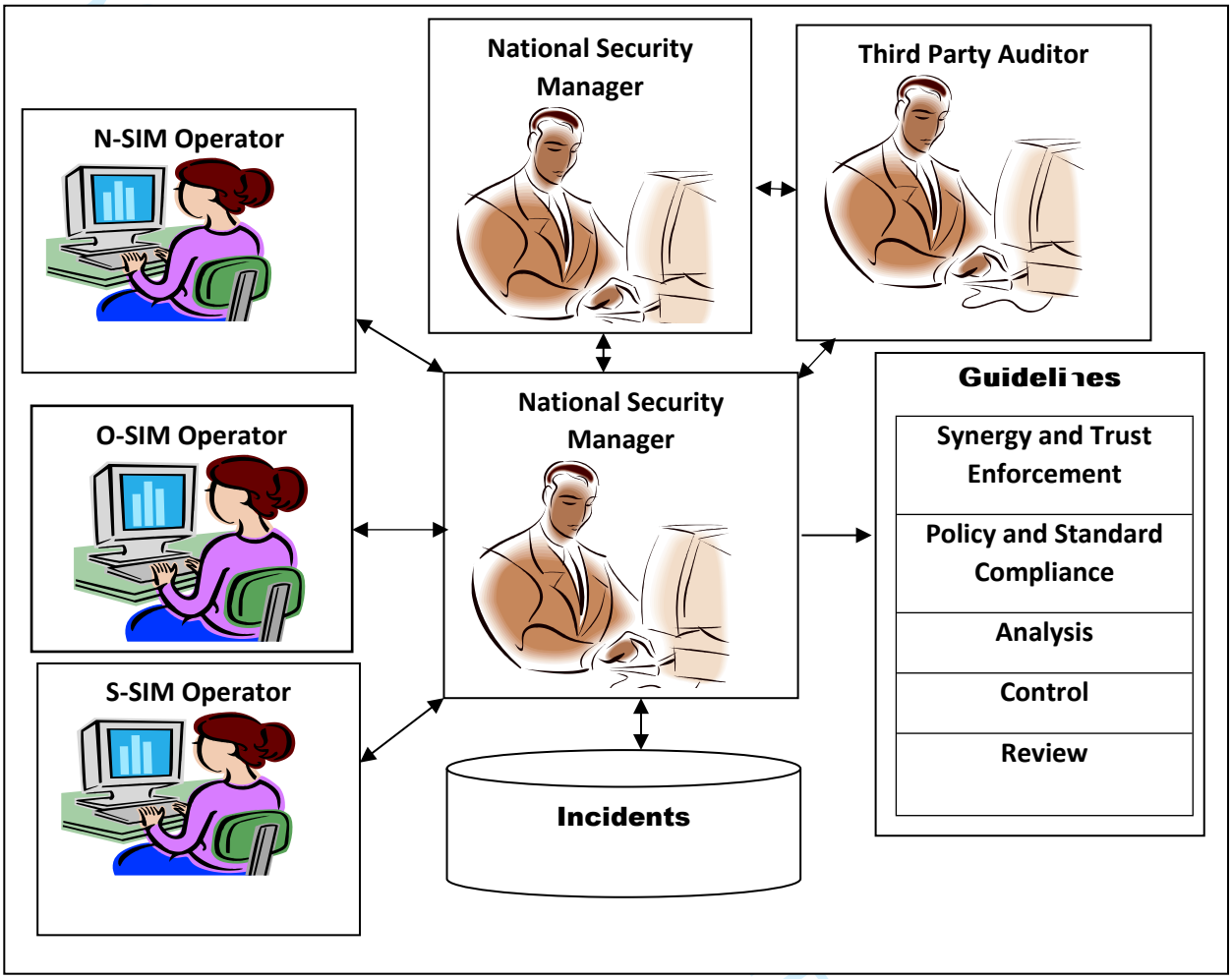

Fig. 2: National Control Unit

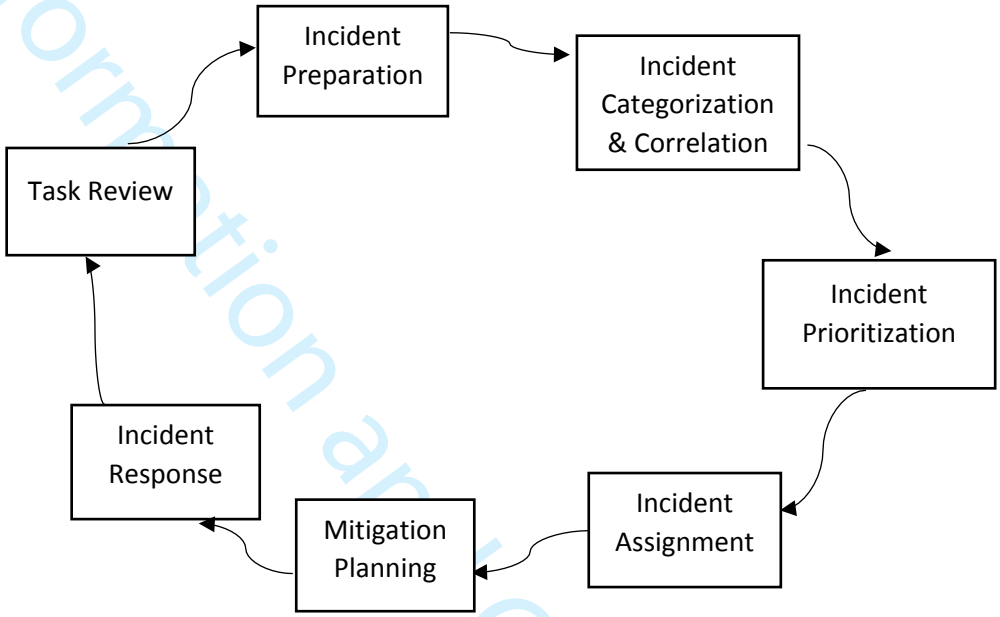

Fig. 3. Security Incident Management Process Lifecycle

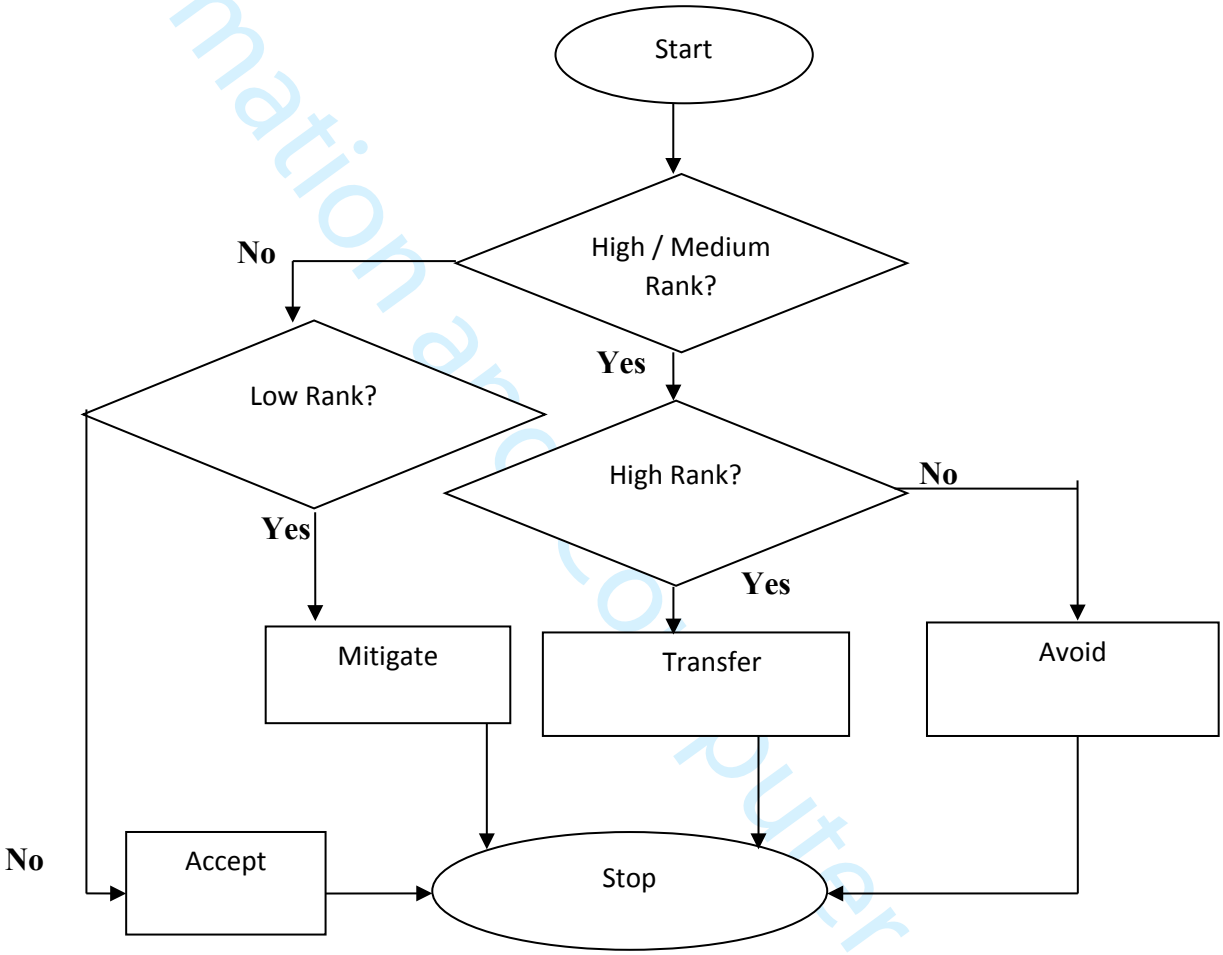

Fig 4. System Flow Chart for Mitigation Planning

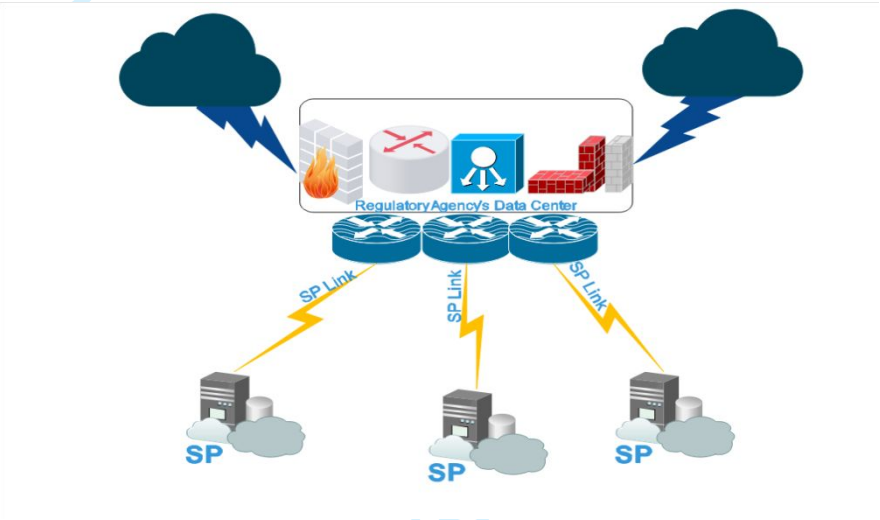

Fig. 5: Structure of the Data Centre Interconnectivity

RealTime Events | Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	15	student-...	3.28929	2014-07-21 19:47:42	10.1.0.134		10.1.0.131		1	GPL ICMP_INFO PING *NIX
RT	60	student-...	3.28947	2014-07-21 19:47:42	10.1.0.134	49163	10.1.0.3	445	6	ET NETBIOS Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
RT	14	student-...	3.28959	2014-07-21 19:47:42	10.1.0.3	8080	10.1.0.135	49162	6	ET CURRENT_EVENTS landing page with malicious Java applet
RT	2	student-...	3.28960	2014-07-21 19:47:42	10.1.0.135	49163	10.1.0.3	8080	6	ET POLICY Vulnerable Java Version 1.7.x Detected
RT	39	student-...	3.28961	2014-07-21 19:47:42	10.1.0.3	8080	10.1.0.135	49163	6	ET INFO JAVA - Java Archive Download By Vulnerable Client
RT	70	student-...	3.28963	2014-07-21 19:47:42	10.1.0.3	8080	10.1.0.135	49163	6	ET CURRENT_EVENTS Possible Metasploit Java Exploit
RT	64	student-...	3.28966	2014-07-21 19:47:42	10.1.0.3	8080	10.1.0.135	49163	6	ET CURRENT_EVENTS Possible Metasploit Java Payload
RT	80	student-...	3.28970	2014-07-21 19:47:42	10.1.0.3	1024	10.1.0.135	49164	6	ET TROJAN Metasploit Meterpreter stdapi_* Command Request
RT	24	student-...	3.28971	2014-07-21 19:47:42	10.1.0.135	49164	10.1.0.3	1024	6	ET TROJAN Metasploit Meterpreter stdapi_* Command Response
RT	2	student-...	3.29056	2014-07-21 19:47:43	10.1.0.166	49167	10.1.0.3	8080	6	ET POLICY Vulnerable Java Version 1.7.x Detected
RT	22	student-...	3.29084	2014-07-21 19:47:43	10.1.0.166	49169	10.1.0.3	1024	6	ET TROJAN Metasploit Meterpreter stdapi_* Command Response
RT	4	student-...	3.29092	2014-07-21 19:47:43	10.1.0.134	49177	10.1.0.133	445	6	GPL NETBIOS SMB-DS IPC$ unicode share access
RT	2	student-...	3.29122	2014-07-21 19:47:43	10.1.0.197	49172	10.1.0.3	8080	6	ET POLICY Vulnerable Java Version 1.7.x Detected
RT	18	student-...	3.29150	2014-07-21 19:47:43	10.1.0.197	49174	10.1.0.3	1024	6	ET TROJAN Metasploit Meterpreter stdapi_* Command Response
RT	1	student-...	3.29159	2014-07-21 19:47:43	10.1.0.3	1024	10.1.0.197	49174	6	ET TROJAN Metasploit Meterpreter core_channel_* Command Request
RT	1	student-...	3.29160	2014-07-21 19:47:43	10.1.0.197	49174	10.1.0.3	1024	6	ET TROJAN Metasploit Meterpreter core_channel_* Command Response
RT	15	student-...	3.29511	2014-07-21 19:47:45	10.1.0.226	23793	10.1.0.3	139	6	GPL NETBIOS SMB IPC$ unicode share access
RT	30	student-...	3.29510	2014-07-21 19:47:45	10.1.0.226	23793	10.1.0.3	139	6	GPL NETBIOS SMB Session Setup NTMLSSP unicode asn1 overflow attempt
RT	16	student-...	3.29595	2014-07-21 19:47:46	10.1.0.35		10.1.0.133		1	GPL ICMP_INFO PING *NIX
RT	1	student-...	3.29624	2014-07-21 19:47:46	10.1.0.134	17500	10.1.0.255	17500	17	ET POLICY Dropbox Client Broadcasting
RT	12	student-...	3.29877	2014-07-21 19:47:47	10.1.0.3	8080	10.1.0.194	27505	6	ET INFO JAVA - Java Archive Download

IP Resolution | Agent Status | Sport Statistics | System Msgs | User Msgs

Search Packet Payload | Hex | Text | NoCase

Fig. 6. Sample Alerts

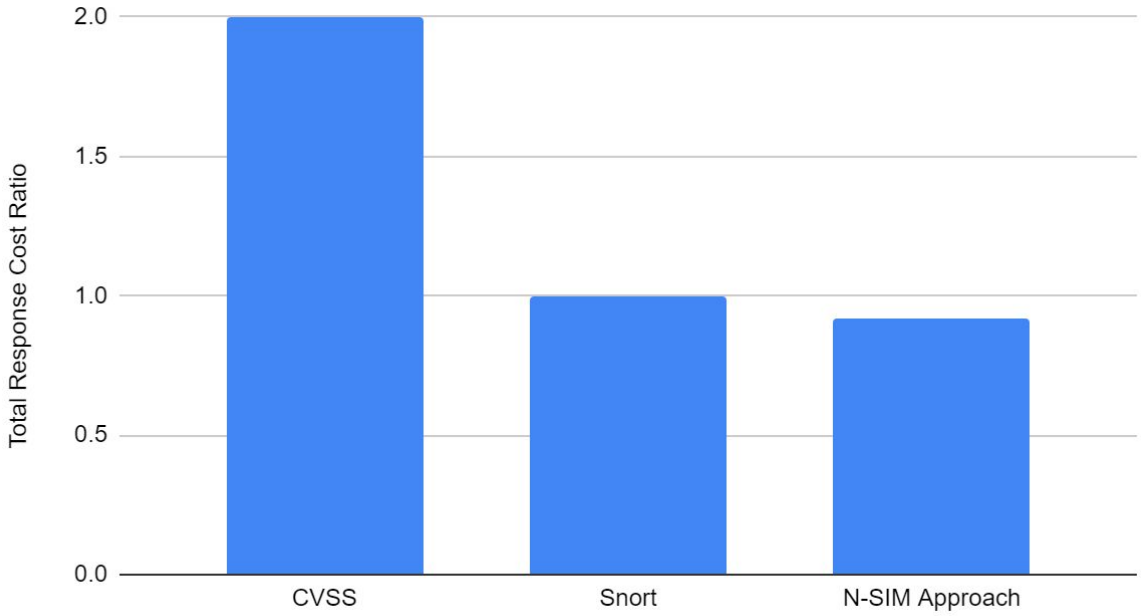

Fig. 7. Total Response Cost for First Attack Scenario in Comparison with Snort

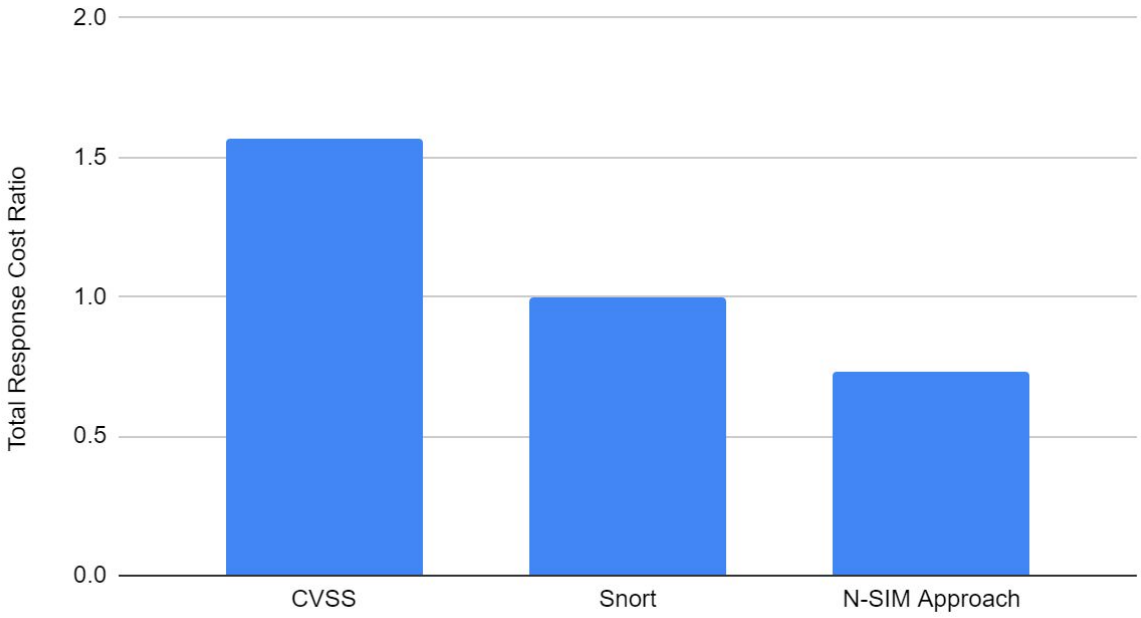

Fig. 8. Total Response Cost for Second Attack Scenario in Comparison with Snort

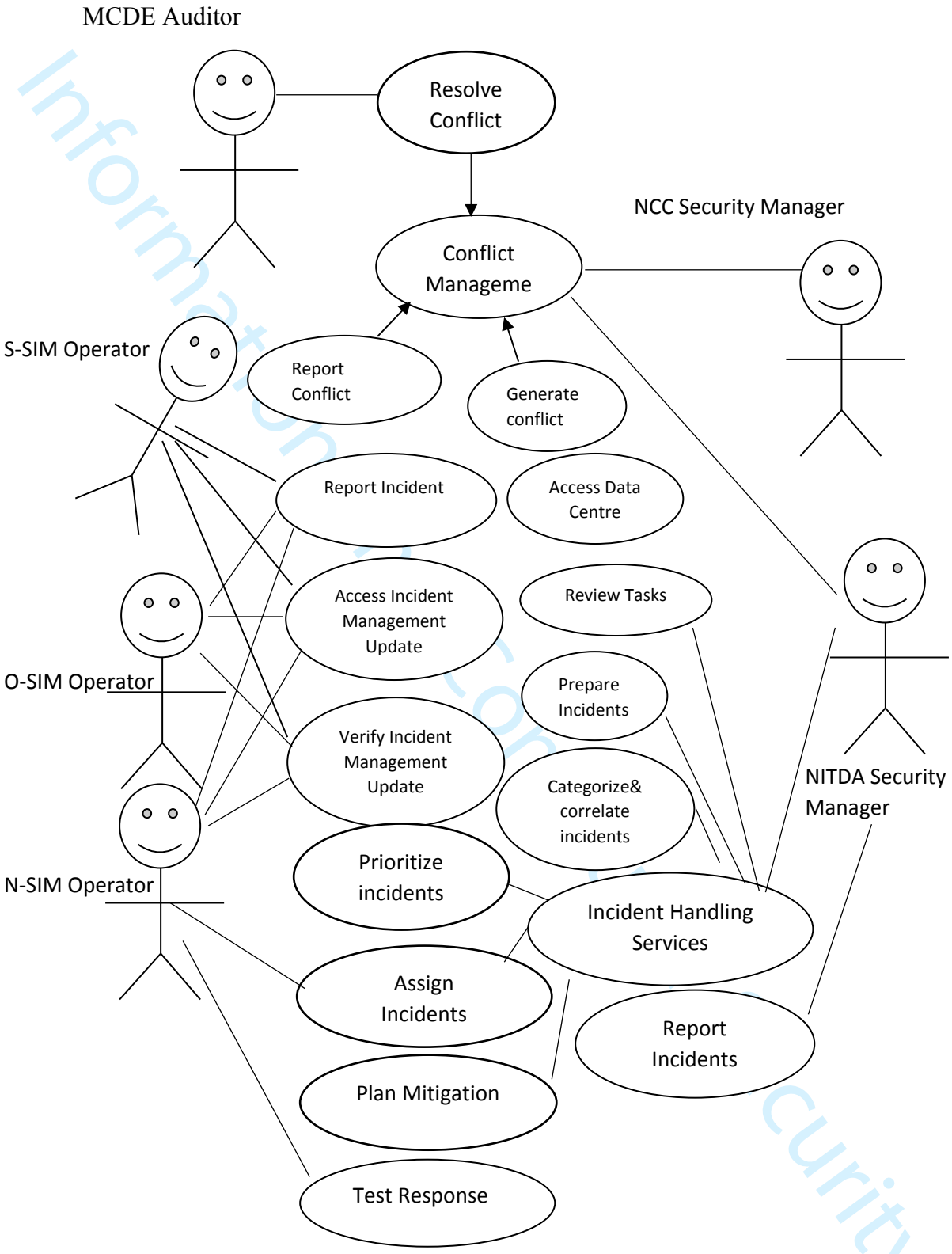

Fig. 9. Use Case for Cybersecurity Incident Management in Nigerian ICT Ecosystem

Table 1: Structured of Incident-related Information

S/N	Category	Feature	Description
1	Incident	Incident_Name	Popular name of the Incident
		Incident_ID	The ID assigned to this incident
		Alternative_ID	The ID numbers used by other sources to refer to the incident described in the document
		Related Activity	The ID numbers of the incidents linked to the one described in this document
		Start_Time	Time at which the incident started.
		End_Time	Time at which the incident ended.
		Detect_Time	Time at which the incident was first detected
		Report Time	The time the incident was reported
		Source_Port	The traced port where incident originate
		Source_IP	The traced IP where incident originate
		Dest_Port	The victim's port
		Dest_IP	The victim's IP
2	System Data	Asset	Name of the server or package
		Asset Category	Category of the Asset
		InfoSec	Name of Information Security Products
		InfoSec Configuration	Configuration of InfoSec device
3	Vulnerability Sources	Vulnerability	Asset Vulnerability Information
		Weakness	Asset Weakness Information
4	User	Contact	Contact Address of Operator
		History	A log of the events or the significant actions which took place during the incident management.
		Additional Information	Mechanism which extends the data model.

Table 2: Trust Classes, Indicators and their Descriptions

Classes	Indicators	Description	Value
S-SIM & O-SIM operators	1. Integrity	It is defined as the extent to which a trustee is believed to adhere to ethical principles.	0 to 0.1
	2. Ability	It captures the "can-do" component of trustworthiness by describing whether the trustee has the skills needed to act in an appropriate fashion.	0 to 0.1
	3. Benevolence	It is the extent to which a trustee is believed to want to do good for the trustor.	0 to 0.1
	4. Trust_Propensity	It is the dispositional trust that is associated to what the actor 'will do' instead of 'can do'.	0 to 0.1
Communication Media	5. Confidentiality	It measures the state of contact medium in ensuring that only those with sufficient privileges and demonstrated need access certain information.	0 to 0.1
	6. Integrity	It is the state of wholeness of contact medium.	0 to 0.1
	7. Availability	It measures the state of contact medium in ensuring uninterrupted user access.	0 to 0.1
Data Source (information security devices and other incident sources)	8. Integrity	This is the measure of the condition of data source to produce the right output.	0 to 0.1
	9. Comprehension	This is the measure of the condition of data source to produce understandable outputs.	0 to 0.1
	10. Reliability	This is the measure of the condition of data source to always produce the right output.	0 to 0.1

Table 3: Attacker-centric Perspectives, Criteria and Scales

Perspective	Criterion	Low Scale (Score = 1)	Moderate Scale (Score = 2)	High Scale (Score = 3)
Exploitability	Exploit Availability	Unavailable	Scarce	Readily
	Ease of Exploitation	Expert	Trained	Novice
Risk of Exposure	Discoverability	Year	Month	Day
	Remediation	Adequate	Inadequate	Unavailable
Damage	Confidentiality Impact	None	Partial	Fully
	Integrity Impact	None	Partial	Fully
	Availability Impact	None	Partial	Fully

Table 4: Victim-centric Perspectives, Criteria and Scales

Perspective	Criterion	Low Scale (Score = 1)	Moderate Scale (Score = 2)	High Scale (Score = 3)
Frequency	Security Device 1	Low	Moderate	High
	Security Device 2	Low	Moderate	High
	. . .	…	…	…
	Security Device N	Low	Moderate	High
Resistance (Inverse of Sensitivity)	Security Device 1	Low	Moderate	High
	Security Device 2	Low	Moderate	High
	. . .	…	…	…
	Security Device N	Low	Moderate	High
Severity	Security Device 1	Low	Moderate	High
	Security Device 2	Low	Moderate	High
	. . .	…	…	…
	Security Device N	Low	Moderate	High

Table 5: Attack Stages for First Attack Scenario

Stage	Host	Attack
1	10.1.0.135	Current_Events Possible Metasploit Java Exploit
2	10.1.0.197	Trojan Metasploit Meterpreter Core_Channel_Command Request
3	10.1.0.135	Trojan Metasploit Meterpreter stdapi_Command Request
4	10.1.0.135	Current_Events landing page with malicious Java Applet
5	10.1.0.135	Current_Events Possible Metasploit Java Payload
6	10.1.0.135	Info Java_Java Archive Download by Vulnerable Clients

Table 6: Attack Stages for Second Attack Scenario

Stage	Host	Attack
1	172.16.113.105	INFO PING NIX
2	172.16.113.105	INFO PING BSD type
3	172.16.114.169	INFO PING NIX
4	172.16.114.169	INFO PING BSD type
5	172.16.112.207	POLICY PE EXE/DLL Windows File Download
6	172.16.112.20	Exploit MS_SQL DOS ATTEMPT (08)
7	172.16.112.100	NETBIOS NT NULL Session
8	172.16.112.100	NETBIOS NT NULL Session
9	172.16.112.105	SNMP Public Access UDP
10	172.16.115.20	RPC PORTMAP SADMIND REQUEST UDP
11	172.16.115.20	RPC Sadmind query with root credentials
12	172.16.113.204	ICMP PING NIX

Table 7: Incident Prioritization Results for N-SIM Approach, CVSS, and Snort for First Attack Scenario

S/N	Incident	N-SIM	CVSS	Snort
1	Current_events Possible Metasploit Java Exploit	6.50 (Low)	(None)	2 (Low)
2	Trojan Metasploit Meterpreter core_channel Command Request	4.04 (Very Low)	(None)	2 (Low)
3	Trojan Metasploit Meterpreter stdapi_command Request	6.00 (Low)	(None)	2 (Low)
4	Current_events landing page with malicious Java Applet	5.00 (Low)	(None)	2 (Low)
5	Current_events Possible Metasploit Java Payload	5.50(Low)	(None)	2 (Low)
6	Info Java_Java Archive Download by Vulnerable Clients	5.50 (Low)	(None)	2 (Low)

Table 8: Incident Prioritization Results for N-SIM Approach, CVSS, and Snort for Second Attack Scenario

S/N	Incident	N-SIM	CVSS	Snort
1	INFO PING NIX	1.75(Very Low)	(None)	3 (Medium)
2	INFO PING BSD type	1.75 (Very Low)	(None)	3 (Medium)
3	INFO PING NIX	1.75 (Very Low)	(None)	3 (Medium)
4	INFO PING BSD type	1.75 (Very Low)	(None)	3 (Medium)
5	POLICY PE EXE/DLL Windows File Download	1.75 (Very Low)	(None)	2 (Low)
6	Exploit MS_SQL DOS ATTEMPT (08)	9.83 (Medium)	8 (High) (CVE:2002-0649)	1 (Very Low)
7	NETBIOS NT NULL Session	4.06(Very Low)	10 (Critical) (CVE:2000-0347	2 (Low)
8	NETBIOS NT NULL Session	11.17(Medium)	10 (Critical) (CVE:2000-0347)	2 (Low)
9	SNMP Public Access UDP	5.42 (Low)	10 (Critical) (CVE:2002-0013)	2 (Low)
10	RPC PORTMAP SADMIND REQUEST UDP	13.00 (High)	10 (Critical) (CVE:2003-0722)	2 (Low)
11	RPC SADMIND Query with root credentials	11.33 (Medium)	0 (None)	2 (Low)
12	ICMP PING NIX	3.50 (Very Low)	0 (None)	3 (Medium)

Table 9: Analysis of the Response Costs for the First Attack Scenario

S/N	Incident	Response	N-SIM (USD)	CVSS (USD)	Snort (USD)
1	Current_events Possible Metasploit Java Exploit	Avoid	0	40	0
		Transfer	0	0	0
		Mitigate	20	0	20
		Accept	0	0	0
		Cost	**20**	**40**	**20**
2	Trojan Metasploit Meterpreter core_channel Command Request	Avoid	0	40	0
		Transfer	0	0	0
		Mitigate	0	0	20
		Accept	10	0	0
		Cost	**10**	**40**	**20**
3	Trojan Metasploit Meterpreter stdapi_command Request	Avoid	0	40	0
		Transfer	0	0	0
		Mitigate	20	0	20
		Accept	0	0	0
		Cost	**20**	**40**	**20**
4	Current_events landing page with malicious Java Applet	Avoid	0	40	0
		Transfer	0	0	0
		Mitigate	20	0	20
		Accept	0	0	0
		Cost	**20**	**40**	**20**
5	Current_events Possible Metasploit Java Payload	Avoid	0	40	0
		Transfer	0	0	0
		Mitigate	20	0	20
		Accept	0	0	0
		Cost	**20**	**40**	**20**
6	Info Java_Java Archive Download by Vulnerable Clients	Avoid	0	40	0
		Transfer	0	0	0
		Mitigate	20	0	20
		Accept	0	0	0
		Cost	**20**	**40**	**20**
	Total Response Cost		**110**	**240**	**120**

Table 10: Analysis of the Response Costs for the Second Attack Scenario

S/N	Incident	Response	N-SIM (USD)	CVSS (USD)	Snort (USD)
1	INFO PING NIX	Avoid	0	40	0
		Transfer	0	0	0
		Mitigate	0	0	30
		Accept	10	0	0
		Cost	**10**	**40**	**30**
2	INFO PING BSD type	Avoid	0	40	0
		Transfer	0	0	0
		Mitigate	0	0	30
		Accept	10	0	0
		Cost	**10**	**40**	**30**
3	INFO PING NIX	Avoid	0	40	0
		Transfer	0	0	0
		Mitigate	0	0	30
		Accept	10	0	0
		Cost	**10**	**40**	**30**
4	INFO PING BSD type	Avoid	0	40	0
		Transfer	0	0	30
		Mitigate	0	0	0
		Accept	10	0	0
		Cost	**10**	**40**	**30**
5	POLICY PE EXE/DLL Windows File Download	Avoid	0	40	0
		Transfer	0	0	0
		Mitigate	0	0	20
		Accept	10	0	0
		Cost	**10**	**40**	**20**
6	Exploit MS_SQL DOS ATTEMPT (08)	Avoid	0	0	0
		Transfer	30	30	0
		Mitigate	0	0	0
		Accept	0	0	10
		Cost	**30**	**30**	**10**
7	NETBIOS NT NULL Session	Avoid	0	40	0
		Transfer	0	0	0
		Mitigate	0	0	20
		Accept	10	0	0
		Cost	**10**	**40**	**20**
8	NETBIOS NT NULL Session	Avoid	0	40	0
		Transfer	30	0	0
		Mitigate	0	0	20
		Accept	0	0	0
		Cost	**30**	**40**	**20**
9	SNMP Public Access UDP	Avoid	0	40	0
		Transfer	0	0	0
		Mitigate	20	0	20

		Accept	0	0	0
		Cost	**20**	**40**	**20**
10	RPC PORTMAP SADMIND REQUEST UDP	Avoid	40	40	0
		Transfer	0	0	0
		Mitigate	0	0	20
		Accept	0	0	0
		Cost	**40**	**40**	**20**
11	RPC SADMIND Query with root credentials	Avoid	0	40	0
		Transfer	30	0	0
		Mitigate	0	0	20
		Accept	0	0	0
		Cost	**30**	**40**	**40**
12	ICMP PING NIX	Avoid	0	40	0
		Transfer	0	0	30
		Mitigate	0	0	0
		Accept	10	0	0
		Cost	**10**	**40**	**30**
	Total Response Cost		**220**	**470**	**300**

Table 9: Performance Comparison Chart for National Cybersecurity Incident Management Set-ups

Evaluation Factors	Proposed Collaborative Approach	Settani *et al.* (2017)	Puuska *et al.* (2018)
Is there a Synergy among the ICT players?	Yes	Yes	Yes
Is there a measure to ensure data trust?	Yes	Yes	Yes
Does the trust capture the reputation of the incident?	Yes	No	Yes
Are standard guidelines and tools used?	Yes	Yes	Yes
Are the analysis models in-depth?	Yes	Yes	No
Does the analysis support divergent incident views?	Yes	Not reported	Yes
Is any case study presented?	Yes	Yes	Yes
Is the scenario evaluated?	Yes	No	Yes
Are there rules of control?	Yes	Yes	Yes
How many regulators are supported?	Multiple	Single	Single
If regulators are multiple, is there a measure to ensure synergy?	Yes	-	-
If regulators are multiple, is there a measure to ensure resolve conflict?	Yes	-	-
Does the architecture support review?	Yes	Yes	Yes